1. Показатель, к которому принадлежит вычет. Свойства.

Показатель, к которому принадлежит вычет

Определение

Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}_p$, $a \neq 0$, $d \in \mathbb{N}$. Вычет a *принадлежит к показателю* d, если $a^d = 1$, но $a^s \neq 1$ при $s \in \mathbb{N}$, $s < d$.
Обозначение: $a \in_p d$.

$Z_5 = \{0, 1, 2, 3, 4\}$

$2^1 = 2;\ 2^2 = 4;\ 2^3 = 3;\ 2^4 = 1$, то есть вычет 2 принадлежит к показателю 4

$3^1 = 3;\ 3^2 = 4;\ 3^3 = 2;\ 3^4 = 1$, то есть вычет 3 принадлежит к показателю 4

Лемма 1

Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}_p$. Тогда выполнены следующие утверждения.

1) *Если $a^d = 1$ и $a \in_p s$, то $s \mid d$.*

2) *Если $a \in_p d$, то $d \mid p - 1$.*

Доказательство. 1) • Предположим противное и поделим d на s с остатком: $d = sq + r$, $0 < r < s$.

• Тогда $1 = a^d = a^{sq+r} = (a^s)^q \cdot a^r = a^r$,

что противоречит минимальности s.

2) По теореме Эйлера $a^{p-1} = 1$. Тогда по пункту 1 имеем $d \mid p - 1$. □

Важным следствием теоремы Эйлера для случая простого модуля является малая теорема Ферма:

Если a не делится на простое число p, то $a^{p-1} \equiv 1 \pmod{p}$.

2. Количество корней многочлена $t^d - 1$ в $\mathbb{Z}_p$, где $p - 1 \vdots d$.

Лемма 2

Если $p \in \mathbb{P}$ и $d \mid p-1$, то многочлен $t^d - 1 \in \mathbb{Z}_p[t]$ имеет ровно d корней, все они не 0.

Доказательство. • Многочлен $t^{p-1} - 1$ имеет в $\mathbb{Z}_p[t]$ ровно $p - 1$ корень (по теореме Эйлера, все ненулевые вычеты его корни).

Теорема 15

Пусть $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Тогда $a^{\varphi(m)} \equiv 1 \pmod{m}$

Важным следствием теоремы Эйлера для случая простого модуля является малая теорема Ферма

> Если a не делится на простое число p, то $a^{p-1} \equiv 1 \pmod{p}$.

$t^{p-1} = 1$ в $Z_p[t]$

$t^{p-1} - 1 = 0$ в $Z_p[t]$

$t^4 - 1 = (t^2+1)(t^2-1) = (t^2+1)(t-1)(t+1); p = 5$

Какие тут корни: $t = 1; t = -1 = 4; t = 2; t = 3$

• Пусть $p - 1 = qd$. Тогда
$t^{p-1} - 1 = (t^d - 1)(t^{(q-1)d} + \cdots + t^d + 1) =: (t^d - 1)f(t)$.

• Так как $\deg(f) = (q-1)d$, этот многочлен по Теореме 3.7 имеет не более $(q-1)d$ корней.

Теорема 7

Пусть K — поле, $f \in K[t]$, $\deg(f) = n$, $\alpha_1, \ldots, \alpha_k \in K$ — все различные корни f, причем корень α_i имеет кратность m_i. Тогда:

1) $f(t) \vdots \prod_{i=1}^{k} (t - \alpha_i)^{m_i}$;
2) $m_1 + \cdots + m_k \le n$. *В частности, $k \le n$.*

• Если $t^d - 1$ имеет менее d корней, то $t^{p-1} - 1 = (t^d - 1)f(t)$ имеет менее $d + (q-1)d = p - 1$ корней, противоречие. $\square$

3. Количество вычетов, принадлежащих к показателю d.

Теорема 1

Если $p \in \mathbb{P}$ и $d \mid p-1$, то к показателю d принадлежит ровно $\varphi(d)$ вычетов.

Доказательство. • Индукция по d. База $d = 1$ очевидна: $a \in_p 1 \iff a = 1$.

Пусть $p = 5$. То есть $Z_p = \{0, 1, 2, 3, 4\}$

$4 \vdots 1; 4 \vdots 2; 4 \vdots 4$

К показателю d должно принадлежать $\varphi(4) = 2$ вычета

$a^1 - 1 = 0; a = 1$

$a^2 - 1 = 0; a = 1$ и $a = 4$

$a^4 - 1 = 0; a = 1$ и $a = 4$

То есть к показателю d принадлежит 2 вычета

Доказательство. • Индукция по d. База $d = 1$ очевидна: $a \in_p 1 \iff a = 1$.

Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}_p$, $a \neq 0$, $d \in \mathbb{N}$. Вычет a *принадлежит к показателю d*, если $a^d = 1$, но $a^s \neq 1$ при $s \in \mathbb{N}$, $s < d$.
Обозначение: $a \in_p d$.

Только одно число в 1-ой степени выдаст 1: собственно 1 ☺

• Все вычеты, принадлежащие к показателю d, являются корнями многочлена $t^d - 1$.

• Если $s \mid d$ (скажем, $d = qs$) и $b \in_p s$, то $b^d = (b^s)^q = 1$, то есть, b — корень $t^d - 1$.

• Так как каждый ненулевой вычет принадлежит в точности одному показателю, вычеты, принадлежащие собственным делителям d дают нам

$$\sum_{s \mid d,\, s<d} \varphi(s) = \left(\sum_{s \mid d} \varphi(s)\right) - \varphi(d) = d - \varphi(d)$$ различных

корней многочлена $t^d - 1$ (последнее равенство верно по Теореме 2.17).

Вычли $\varphi(d)$, потому что d = s – это делитель d. А d в свою очередь – делитель p-1. А мы считаем собственные делители d.

Теорема 17

Для любого $n \in \mathbb{N}$ $\quad \sum\limits_{d \in \mathbb{N},\, d \mid n} \varphi(d) = n.$

• Оставшиеся $d - (d - \varphi(d)) = \varphi(d)$ корней многочлена $t^d - 1$ принадлежат к d (по Лемме 1 они должны принадлежать к делителю d, а этим делителем может быть только само d). □